UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,454	08/31/2000	David Cheriton	CISCP537	3379

26541 7590 12/02/2004

RITTER, LANG & KAPLAN
12930 SARATOGA AE. SUITE D1
SARATOGA, CA 95070

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/652,454	CHERITON, DAVID	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-21 and 23-36* is/are pending in the application.

4a) Of the above claim(s) *31-35* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6-21 and 23-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) *31-35* are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 7/14/04 has been received and considered.

2. Claims 1, 3-4, 6-21 & 23-36 are pending.

Election/Restrictions

3. Newly submitted claims 31-35 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: Claims 31-35 are directed to a network classification system where information about packets classified into network flows are extracted and used to modify further classification, used in congestion control and avoidance. The originally filed claims are directed to a network packet filter or firewall that can generate filters in response to detecting potentially harmful traffic, not requiring reclassifying. Claims 31-35 are related to the originally filed claims as sub-combinations usable together; separate utility is described above, but the inventions are usable together to provide both congestion control and adaptive firewall capabilities. Newly submitted claims 31-35, directed to congestion control require a separate search in classes 709/206-207, 223-224, 229, 234-235 & 239-242.

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 31-35 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Response to Arguments

4. Applicant's arguments with respect to claims 1, 3-4 & 6-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-4, 6-7, 9-11, 15-18, 20-21, 25, 27 & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 97/24841 to Cheriton et al. (Cheriton) in view of U.S. Patent 6,321,338 to Porras et al. (Porras).

Regarding claims 1, 6, 9-10, 15-16, 18 & 36, Cheriton discloses classifying network flows/virtual paths based on one or more packets/datagrams received at the network device (p. 7, ¶2 & p. 8, ¶2-3), performing a lookup for each of the classified network flows/virtual paths (p. 8, ¶2) and building a new flow/virtual path cache entry if the lookup is unsuccessful (p. 8, ¶3), sending each of said network flows/virtual paths to a corresponding flow/virtual path cache (p. 8, ¶3) and implementing policies designated for each of said network flows (p. 13, ¶5). Cheriton lacks creating an aggregate network flow summary for each of said network flows, analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows and generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through said network device. However, Porras teaches a system to enable detection of suspicious activity despite virtual private network

security techniques such as encryption (col. 2, lines 61-64). Porras teaches creating an aggregate network flow summary/statistical profile for each of said network flows/connections/streams (col. 1, line 59 – col. 2, line 18 & col. 14, lines 7-19), analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows (col. 1, line 59 – col. 2, line 18) and generating a filter/countermeasure (col. 12, lines 8-19) to prevent packets corresponding to detected potentially harmful network flows from passing through said network device (col. 2, lines 2-7, col. 5, lines 13-14 & col. 8, lines 53-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include creating an aggregate network flow summary for each of said network flows, analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows and generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through said network device. One of ordinary skill in the art would have been motivated to perform such a modification to enable detection of suspicious activity, as taught by Porras (col. 1, line 59 – col. 2, line 18, col. 2, lines 61-64, col. 5, lines 13-14, col. 8, lines 53-65 & col. 12, lines 8-19).

Regarding claims 3 & 4, Cheriton discloses classifying the network flow base on a source device sending a packet (p. 7, ¶2).

Regarding claim 7, Cheriton lacks propagating a filter to an upstream network device. However, Porras teaches that causing other entities to be alerted about an attack can protect network from global attacks (col. 2, lines 54-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to propagate a filter to an upstream network device. One of ordinary skill in the art would have been motivated to perform

such a modification to cause another entity to be alerted to correlate activity, as taught by Porras (col. 2, lines 54-60).

Regarding claims 11 & 25, Cheriton discloses selecting a class of flows/virtual paths to analyze based on previously analyzed paths (p. 8, ¶2-3).

Regarding claim 27, Cheriton, as modified above, lacks a class of packets being selected for analysis based on statistics associated with an aggregate filter. However, Porras teaches that packets to analyze can be selected on different criteria, possibly to implement application monitoring (col. 5, lines 4-21). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select a class of packets to be analyzed based on statistics associated with the aggregate filter. One of ordinary skill in the art would have been motivated to perform such a modification to implement application monitoring, as taught by Porras (col. 5, lines 4-21).

Regarding claims 17 & 21, Cheriton, as modified above, lacks propagating the filter to an upstream network device. However, Porras teaches that intrusion reports can be propagated to an enterprise monitor (upstream) to sensitize monitors in other domains to the same activity (col. 8, lines 47-65). Further, Porras teaches reports can result in a countermeasure/filter to sever communications (col. 12, lines 8-19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to propagate the filter to an upstream device. One of ordinary skill in the art would have been motivated to perform such a modification to sensitize other domains of the same activity and to sever potentially harmful communications, as taught by Porras (col. 8, lines 47-65 & col. 12, lines 8-19).

Regarding claim 20, Cheriton, as modified above, discloses an ACL classifier/switch hardware (p. 13, ¶4 & Fig. 4), a lookup device/virtual path cache (p. 13, ¶4 & Fig. 4) and a plurality of flow buckets/shared buffer memory (p. 13, ¶3-4 & Fig. 4).

7. Claims 8 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claims 1 & 18 above, in further view of U.S. Patent 6,266,706 to Brodnik et al. (Brodnik). Cheriton, as modified above, lacks the sending step being performed in hardware and the analyzing step being performed by software. However, Brodnik teaches that special-purpose hardware is useful for high-speed and software is used for flexibility (col. 2, line 64 – col. 3, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system so the sending step is performed in hardware and the analyzing step is performed by software. One of ordinary skill in the art would have been motivated to perform such a modification to make the sending step fast and the analyzing step flexible to change, as taught by Brodnik (col. 2, line 64 – col. 3, line 3).

8. Claims 12 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claim 1 above, in further view of U.S. Patent 6,789,203 to Belissent. Cheriton, as modified above, lacks denial of service attacks. However, Belissent teaches that denial of service attacks deprive an organization of services and are usually identified and block accordingly (col. 2, lines 1-32). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to consider denial of service attacks as potentially harmful. One of ordinary skill in the art would have been motivated to perform such

a modification to avoid organizations from being deprived of services, as taught by Belissent (col. 2, lines 1-32).

9. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claim 1 above, in further view of U.S. Patent 6,389,532 to Gupta et al. (Gupta). Cheriton, as modified above, lacks explicitly identifying a source address associated with a harmful network flow and generating a filter to prevent packets from that source from passing through the network. However, Gupta teaches that a router can filter packets when a predetermined router limit, such as a rate at which a router may receive packets form a particular source, has been exceeded, to prevent denial of service attacks (col. 7 lines 28-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify a source of a harmful packet flow and generate a filter to prevent incoming packets from the source. One of ordinary skill in the art would have been motivated to perform such a modification to prevent denial of service attacks, as taught by Gupta (col. 7 lines 28-52).

10. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claim 1 above, in further view of "Live Traffic Analysis of TCP/IP Gateways" by Valdes et al. (Valdes), in further view of Brodnik. Cheriton, as modified above, lacks reducing the flow summaries in hardware so that the flow records can be analyzed by software. However, Valdes teaches that filtering out uninteresting results in a decision unit can make analysis response more manageable (§7, ¶1-2). Further, Brodnik teaches that special-purpose hardware is useful for high-speed and software is used for flexibility (col. 2, line 64 –

col. 3, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reduce flow summaries in hardware. One of ordinary skill in the art would have been motivated to perform such a modification to make analysis response more manageable, as taught by Valdes (§7, ¶1-2) and to make the reduction step faster, as taught by Brodnik (col. 2, line 64 – col. 3, line 3).

11. Claims 24 & 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claim 1 above, in further view of "Application Note 2037 Nemesis Firewall" by Allied Telesyn. Cheriton, as modified above, lacks refining said filter. However, Allied Telesyn teaches that it is known in the art to refine the security policy/rules in a firewall because the default options are not specific (page 4, § Rules and Policies). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to refine the rules/policies. One of ordinary skill in the art would have been motivated to perform such a modification to personalize the filtering rather than using the defaults of a firewall/packet filter, as taught by Allied Telesyn (page 4, § Rules and Policies).

12. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton & Porras, as applied to claim 1 above, U.S. Patent 6,651,099 to Dietz et al. (Dietz). Cheriton, as modified above, lacks sending information on a selected group of flows to a classifier. However, Dietz teaches that to recognize a conversational flow associated with a particular applications, it is necessary to examine further packets and maintain a state of a flow (col. 10, lines 8-23). Packets are continually reclassified until a conversational flow (as opposed to a connection flows

(col. 2, lines 34-48)) is satisfactorily identified (col. 10, lines 8-35). Conversational flow recognition is useful because a single application may produce different "connection flows" (col. 3, lines 34-48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to pass information on the selected group of network flows to a classifier. One of ordinary skill in the art would have been motivated to perform such a modification to recognize conversational flows, as taught by Dietz (col. 2, lines 34-48 & col. 10, lines 8-35).

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
November 16, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100